REMARKS

In an Office Action mailed 13 December 2005, the Examiner rejected claims 1, 2, 5, and 8 under 35 USC §102(b) as being anticipated by Fielder et al. (US Patent No. 6,049,612, hereinafter "Fielder Patent"), and claims 3, 4, 6, and 7 under 35 USC §103(a) as being unpatentable over Fielder as applied to claims 1 and 5 above, and further in view of Kudo et al. (US Patent No. 6,381,695, hereinafter "Kudo Patent"). The Examiner noted with respect thereto:

> Fielder discloses a method for generating an encryption key comprising:
> retrieving the host identification from the host device (4:29-31 wherein the E-Key Seed acts as the host identification (6:13-15);
> generating at least one content variable (4:29-31 wherein the constant value is the content variable);
> combining the host identification and the at least one content variable to produce two or more combinations, wherein the method used to combine the host identification and the at least one content variable repeatedly produces the same two or more combinations (5:18-30); and
> coalescing the two or more combinations to produce the encryption key, wherein the method of coalescing the two or more combinations repeatedly produces the same encryption key (5:18-30).

Applicants have reviewed the cited Fielder Patent and the Examiner's clearly stated grounds of rejection, and has amended claims 1 – 8 and added claims 9 – 11 in response thereto. Applicants provide the following remarks in support of patentability of these amended and newly added claims.

The present method for encryption key generation provides a method of combining the speed of conventional encryption with the security of public key encryption. The host device encrypting the plaintext to be transmitted over the unsecured interface is assigned a host identification. The host identification is stored in a secure location within the host device. The host identification is analogous to the private key. Only the host device can generate the encryption key used to later decrypt the ciphertext. A second variable, a content identification, is generated by the host device. Each successive block of plaintext to be encrypted uses a different content identification. The host identification along with the content identification is used for generating an encryption key to encrypt a block of plaintext. This second variable, the content identification, is analogous to the public key. The content identification is transmitted with the resulting ciphertext and, together, the ciphertext and content identification are stored for retrieval at a later time. The encryption key is generated following a method that can be repeated later using the same host identification and content identification to generate the same encryption key. In other words, the formula used to generate the encryption key is deterministic.

This structure is recited in Applicant's independent claim 1 as follows:

> A method for generating an encryption key for use with a host device having a host identification stored therein, for encryption a file comprising a plurality of blocks of plaintext data in a manner that said encrypted file can only be decrypted by said host device, the method comprising:
> retrieving the host identification from the host device for use as a private portion of an encryption key;
> generating at least one content variable that uniquely identifies a corresponding block of said file as a public portion of said encryption key;
> combining the host identification and the at least one content variable to produce the encryption key;
> encrypting a block of plaintext data using the encryption key to produce a block of ciphertext;
> appending only the at least one content variable to the block of ciphertext; and
> storing the block of ciphertext and the appended one or more content variable within a storage device.

In contrast, the Fielder patent discloses:

> A system for protecting sensitive information files and messages from access by unauthorized parties, whether stored in a computer memory or exchanged over a transfer medium between sending and receiving stations. Each document or message file is created in normal operation. A constant value or message is logically combined to a secret bit sequence (E-Key Seed) to perform a many-to-few bit mapping which shuffles the bits and provides a pseudo-random result. The result then is applied through a secure hash function generator to perform a second many-to-few bit mapping and provide a pseudo-random message digest. The message digest in turn may be truncated to a desired bit length to provide a deterministic but non-predictable, pseudo-random, symmetric encryption key which is used to encrypt the message or information file to be protected. The deterministic encryption key is destroyed immediately after use. The constant value and encrypted message thereupon are secure hashed to create a message integrity code (MIC) that is used to detect any alterations to the encrypted information file that may have occurred intentionally or unintentionally.

The Fielder patent fails to show or suggest creating an encryption key using data that is part public and part private, using the encryption key to code a file, then storing only the public portion of the data that is used to create the encryption key with the coded file, such that only the host device that encrypted the file can decrypt the file because it is the only one that has the private portion of the data used to generate the encryption key.

Therefore, Applicants believe that claims 1 – 11 are allowable under 35 USC §102(b) and 35 USC §103(a) over the cited references.

In view of the above amendments and remarks, Applicants believe the pending application is in condition for allowance. Applicants believe no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-1848, under Order No. 013208.0121PTUS from which the undersigned is authorized to draw.

Respectfully submitted,
PATTON BOGGS LLP

Dated: 13 MAR 2006

By: _____
Varen C. Belair
Registration No.: 49,056
(214) 758-6631
(214) 758-1550 (Fax)
Attorney for Applicants

Customer No. 24283